UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,188	07/30/2001	Keith Alexander Harrison	30003040-2	2580

7590 01/05/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/918,188	HARRISON ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,7-17,21-37,39-43,48-59 and 63-65* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,7-17,21-37,39-43,48-59 and 63-65* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-2,7-17,21-37,39-43,48-59, and 63-65 have been considered. The examiner notes his appreciation for the applicant's canceling of some of the claims of the previous action in an effort to expedite prosecution of the case, especially in light of the plethora of issues the applicant has presented in the case.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/17/05 has been entered.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 64-65 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. After further consideration, the examiner believes that claims 64 and 65, which were entered as new claims in the amendments filed 5/13/05, should not have been entered because they present new matter which was not described in the originally filed Specification.

Specifically, the examiner finds no support for the following limitation: "decrypting, using a remote device, the encrypted session key using the received intended recipient's public key and an intended recipient's private key residing in the remote device". A specific reference as to where this limitation is disclosed in the Specification or appropriate correction is required.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 21 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. More specifically, the applicant claims "encrypting the session key with the first token" in part b and "decrypting the encrypted session key with the second token" in part f). It is unclear whether or not the session key is encrypted and decrypted using a plurality of tokens or just using one token. Appropriate correction is required.

Claim 63 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim depends on claim 60, which is a cancelled claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 54-56 and 58-59 are rejected under 35 U.S.C. 102(e) as being anticipated by Chan, U.S. Patent No. 6,378,070.

As per claims 54-56 and 58-59, the applicant describes a method of delivering a digital document from a first station via a communications network to an intended recipient at a second station comprising the following limitations which are met by Chan:

a) obtaining details of the intended recipient, including an independently verifiable data record of the intended recipient at the first station (Col 6, line 20- Col 7, line 51);

b) determining prior to transmission of the document whether the second station is one which is arranged to implement the present method (Col 6, line 20- Col 7, line 51);

c) transmitting the document and the independently verifiable data record of the intended recipient to the second station (Col 6, line 20- Col 7, line 51);

d) transmitting the independently verifiable data record of the intended recipient to the second station (Col 6, line 20- Col 7, line 51);

e) receiving and securely retaining the transmitted document and receiving the data record at the second station (Col 6, line 20- Col 7, line 51);

f) obtaining a first part of an intended recipient's identifying token at the second station (Col 6, line 20- Col 7, line 51);

g) requesting proof of the intended recipient's identity at the second station using the transmitted independently verifiable data record (Col 6, line 20- Col 7, line 51);

h) releasing the document to the intended recipient when the intended recipient has proved their identity using a second part of the recipient's identifying token (Col 6, line 20- Col 7, line 51).

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 54-59 are rejected under 35 U.S.C. 102(b) as being anticipated by Mandelbaum, European Patent Application Publication No. 0671830 A2.

As per claim 54, the applicant describes a method of delivering a digital document from a first station via a communications network to an intended recipient at a second station comprising the following limitations which are met by Mandelbaum:

a) obtaining details of the intended recipient, including an independently verifiable data record of the intended recipient at the first station (Col 5, lines 5-11);

b) determining prior to transmission of the document whether the second station is one which is arranged to implement the present method (Col 5, lines 5-11);

c) transmitting the document and the independently verifiable data record of the intended recipient to the second station (Col 5, lines 29-33);

d) transmitting the independently verifiable data record of the intended recipient to the second station (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-26);

e) receiving and securely retaining the transmitted document and receiving the data record at the second station (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-26);

f) obtaining a first part of an intended recipient's identifying token at the second station (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-26);

g) requesting proof of the intended recipient's identity at the second station using the transmitted independently verifiable data record (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-26);

h) releasing the document to the intended recipient when the intended recipient has proved their identity using a second part of the recipient's identifying token (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-26).

As per claim 55, the applicant describes the method according to claims 54, which is met by Mandelbaum, with the following limitation which is also met by Mandelbaum:

Further comprising obtaining details of the intended recipient including the independently verifiable data record prior to transmitting the document (Col 5, lines 5-27).

As per claims 56, the applicant describes the method according to claim 55, which is met by Mandelbaum, with the following limitation which is also met by Mandelbaum:

Wherein the step of obtaining details comprises obtaining the independently verifiable data record from a central database storing many possible intended recipients' details (Col 5, lines 9-11).

As per claim 58, the applicant describes the method of claim 54, which is met by Mandelbaum, with the following limitation which is also met by Mandelbaum:

Further comprising encoding the document prior to transmitting it to the second station and decoding the received document once the intended recipient has proven their identity (Col 5, lines 33-40; Col 7, lines 27-44);

The use of encoding or encrypting the document is described (Col 5, lines 33-40) as is the use of decoding or decrypting the document (Col 7, lines 27-44).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1-2,8-10,13-17,22-24,41-43, and 48-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, U.S. Patent No. 6,378,070, in view of Nishiwaki, U.S. Patent No. 5,602,973.

As per claims 1-2,8-10,13-17,22-24,41-43,48-53, the applicant describes a method of delivering a digital document to an intended recipient comprising the following limitations which are met by Chan in view of Nishiwaki:

a) receiving and securely retaining a transmitted document at the printout station (Chan: Col 7, lines 8-50);

b) receiving an independently verifiable data record of the intended recipient at the printout station (Chan: Col 7, lines 8-10);

c) obtaining a first token of the intended recipient (Chan: Col 7, lines 8-10);

d) requesting proof of the intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient (Chan: Col 7, lines 8-10);

e) releasing the document when the intended recipient has proved their identity by use of a second token that is uniquely related to the first token, wherein the retaining step comprises printing out the document as received and placing it in a locked compartment and the releasing step comprises a controller unlocking the compartment where the printed copy of the document is stored (Nishiwaki: Col 2, lines 6-46).

Chan discloses all the limitations of the above claim, except for printing out the document and placing it in a locked compartment. This idea is disclosed by Nishiwaki. Combining Nishiwaki into the system allows the document to be printed out and placed in a locked compartment. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Nishiwaki with those of Chan because doing so furthers security in the system by incorporating the use of a locked compartment to heighten security in the system.

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chan in view of Nishiwaki in further view of Menezes (Menezes, Alfred J. Handbook of Applied Cryptography. CRC Press. Washington DC. 1997. pages 452-454).

As per claim 7, the applicant describes the method according to claim 1, which is met by Chan in view of Nishiwaki, with the following limitation which is met by Menezes:

Wherein the requesting step comprises requesting supply of data encoded with the second token which can be decoded with the first token (Menezes: pages 452-454);

Chan in view of Nishiwaki discloses all the limitations of claim 1. Chan in view of Nishiwaki also discloses that the user proves his identity by providing supply of data when the document store receives identity information read by the smart card reader and forwarded by the printer (Col 7, lines 1-7).

However, Chan in view of Nishiwaki does not disclose that the supply of data is encoded with the second token (private key) and decoded with the first token (public key). Menezes discloses the idea of a digital signature. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Menezes with those of Chan in view of Nishiwaki and digitally sign the supply of data with the private key because doing so provides a more secure way to authenticate the identity of the user.

Claims 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan in view of Nishiwaki in further view of Schneier (Schneier, Bruce. Applied Cryptography. 1996. John Wiley & Sons, Inc. Second Edition. Pages 68-73, 575-576).

As per claims 11 and 12, the applicant describes the method of claim 1, which is met by Chan in view of Nishiwaki, with the following limitation which is met by Schneier:

Wherein the intended recipient's independently verifiable data record is provided as an intended recipient's digital certificate (Schneier: pages 575-576);

Chan in view of Nishiwaki discloses all the limitations of claim 1. However Chan in view of Nishiwaki does not discloses that the independently verifiable data record is a digital certificate.

Schneier discloses that a certificate can be transmitted between users to verify. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneier with those of Chan in view of Nishiwaki and have a certificate sent as an additional independently verifiable data record so that further verification can be provided and/or a public key of a user can be extracted.

Claims 21,25-37, and 39-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan in view of Carman, U.S. Patent No. 6,272,632.

As per claims 21,25-37, and 39-40, the applicant describes a method of delivering a digital document to an intended recipient at a printout station comprising the following limitations which are met by Chan in view of Carman:

a) obtaining a first token of each intended recipient (Chan: Col 7, lines 8-50; Carman: Col 19, line 62 to Col 20, line 3);

b) encoding the digital document with a session key using a lightweight symmetric cryptographic encryption algorithm, and encrypting the session key with the first token using an encryption algorithm that is more computationally intensive than the symmetric cryptographic encryption algorithm (Chan: Col 7, lines 8-50);

c) receiving and securely retaining the digital document, the encrypted session key and an independently verifiable data record of each intended recipient (Chan: Col 7, lines 8-50);

d) requesting proof of each intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient (Chan: Col 7, lines 8-50);

e) receiving proof of each intended recipient's identity in the form of a second token uniquely related to the first token (Chan: Col 7, lines 8-50);

f) decrypting the encrypted session key with the second token, decoding the digital document with the decrypted session key, and releasing the document (Chan: Col 7, lines 8-50);

g) the receiving step comprises receiving a plurality of transmitted independently verifiable data records of the intended recipients at the printout station (Chan: Col 7, lines 8-50);

h) the obtaining step comprises obtaining the first tokens of each of the intended recipients (Chan: Col 7, lines 8-50);

i) the requesting step comprises requesting proof of each of the intended recipients' identities at the printout station using data in the independently verifiable data records of the intended recipients (Chan: Col 7, lines 8-50);

j) the processing step comprises processing each of the intended recipients' response to the request and releasing the document when all of the intended recipients have proved their identity by use of respective second tokens that are each uniquely related to respective ones of the first tokens (Chan: Col 7, lines 8-50);

Chan discloses the above limitations with the exception that Chan does not disclose obtaining a plurality of first tokens. Chan discloses obtaining only a first token of a single recipient. Carman discloses the idea of obtaining a plurality of first tokens (public keys) to encrypt a message so that a plurality of entities are necessary to play a part in the decryption. Combining the ideas of Carman with Chan allows for a message to be encrypted in more than one first token. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Carman with those of Chan for the purpose of creating an environment which is more secure because it depends on more than one entity providing verification for a received message.

Claims 57 and 63-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan in view of Schneier.

As per claims 57 and 63, the claims are rejected under Chan in view of Schneier for the same reasons given in the rejection of claim 12.

As per claims 64 and 65, the applicant describes a method of delivering a digital document to an intended recipient at a printout station, comprising the following limitations which are met by Chan in view of Schneier:

a) obtaining a public token of the intended recipient (Chan: Col 6, lines 35-40);

b) encrypting the digital document with a session key (Chan: Col 6, lines 20-29);

c) encrypting the session key with the intended recipient's public key (Chan: Col 6, lines 35-38);

d) communicating to the printout station and securely retaining the encrypted digital document at the printout station (Chan: Col 7, lines 21-29);

e) communicating the encrypted session key to the printout station (Chan: Col 7, lines 21-29);

f) communicating an independently verifiable data record of the intended recipient to the printout station, the independently verifiable data record comprising the intended recipient's public key (Chan: Col 7, lines 21-29; Schneier: pages 575-576);

g) communicating the independently verifiable data record comprising the intended recipient's public key to a remote device (Chan: Col 7, lines 21-29);

h) decrypting, using a remote device, the encrypted session key using the received intended recipient's public key and an intended recipient's private key residing in the remote device (Chan: Col 7, lines 21-29);

i) communicating the decrypted session key from the remote device to the printout station (Chan: Col 7, lines 21-29);

j) decrypting, at the printout station, the digital document using the decrypted session key (Chan: Col 7, lines 45-49);

k) releasing the document (Chan: Col 7, lines 50-51).

Claims 1-2,5-11,13-17,41-43,46-48,54-56, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable by Mandelbaum, European Patent Application Publication No. 0671830 A2, in view of Nishiwaki.

As per claims 1,41, and 49, the applicant describes a method of delivering a digital document to an intended recipient at a printout station comprising the following limitations which are met by Mandelbaum in view of Nishiwaki:

a) receiving and securely retaining a transmitted document at the printout station (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-26);

b) receiving an independently verifiable data record of the intended recipient at the printout station (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-26);

b) obtaining a first token of the intended recipient (Mandelbaum: Col 2, lines 50-53);

c) requesting proof of the intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient (Mandelbaum: Col 6, lines 56-58; Col 7, lines 1-6; Col 5, lines 49-58; Table 10 of Fig 4);

d) releasing the document when the intended recipient has proven their identity by use of a second token that is uniquely related to the first token, wherein the retaining step comprises printing out the document as received and placing it in a locked compartment and the releasing step comprises a controller unlocking the compartment where the printed copy of the document is stored (Mandelbaum: Col 7, lines 27-47; Nishiwaki: Col 2, lines 6-46);

Mandelbaum discloses all the limitations of the above claim, except for printing out the document and placing it in a locked compartment. This idea is disclosed by Nishiwaki. Combining Nishiwaki into the system allows the document to be printed out and placed in a locked compartment. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Nishiwaki with those of Mandelbaum because doing so furthers security in the system by incorporating the use of a locked compartment to heighten security in the system.

As per claims 2 and 42, the applicant describes the method of claims 1 and 41, which are anticipated by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Wherein the transmitted document is a fax document and the printout station comprises a fax machine (Col 3, lines 15-17).

As per claim 7, the applicant describes a method according to claim 1, which is anticipated by Mandelbaum in view of Nishiwaki, with the following limitation which is also met by Mandelbaum:

Wherein the requesting step comprises requesting supply of data encoded with the second token which can be decoded with the first token (Col 4, lines 11-21).

As per claim 8, the applicant describes the method of claim 1, which is anticipated by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Wherein the releasing step is carried out when the intended recipient has presented a portable data carrier holding the second token to the printout station and has transferred data to prove their identity (Col 7, lines 27-56).

As per claims 9 and 48, the applicant describes the method of claims 8 and 41, which are met by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Wherein the releasing step further comprises the intended recipient entering a verifiable security identifier into the printout station to establish that they are the legitimate owner of the portable data carrier (Col 4, lines 21-24).

As per claim 10, the applicant describes the method of claim 8, which is met by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Wherein the portable data carrier is a smart card and the printout station comprises a smart card reader (Col 4, lines 9-13).

As per claim 11, the applicant describes the method of claim 1, which is met by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Wherein the obtaining step comprises extracting the first token transmitted with the document and the data record (Table 404 of Fig 4);

As one can see in the table, the fax machine is able to extract information about the first token from the message and display the information as a flag which is set when the message is encrypted with the intended recipient's public key.

As per claim 13, the applicant describes the method of claim 1, which is met by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Further comprising carrying out an on-line check of the validity of the intended recipient's independently verifiable data record (Col 4, lines 17-24);

The applicant writes that the smart card authentication method is preferably the AT&T CSS user authentication system "in which the user calls the system" (Col 4, lines 17-19). Since the user is calling the system for authentication, an online authentication is taking place.

As per claim 14, the applicant describes the method of claim 1, which is met by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Further comprising instructing a third party to carry out an on-line check of the validity of the intended recipient's independently verifiable data record (Col 4, lines 17-24);

Since the authentication system is one in which the user calls into the system, it is reasonable to assume that a third party validates the intended recipient.

As per claims 15 and 16, the applicant describes the method of claims 13 and 14, which are met by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Wherein the releasing step further comprises only releasing the document if the validity of the independently verifiable data record has been confirmed as a result of the check (Col 4, lines 23-24).

As per claims 17,43, and 50-53, the applicant describes the method of claims 1,41, and 49, which are met by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Wherein the first and second tokens comprise private and public encryption/decryption keys of the intended recipient (Col 2, lines 50-53; Col 7, lines 27-32);

The use of the recipient's public key, or first token, is described (Col 2, lines 50-53) as well as the use of the intended recipient's private key, or second token, (Col 7, lines 27-32).

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in view of Nishiwaki in view of Schneier.

As per claim 12, the applicant describes the method of claim 11, which is met by Mandelbaum in view of Nishiwaki, with the following limitation which is met by Schneier:

Wherein the intended recipient's independently verifiable data record is provided as an intended recipient's digital certificate (Schneier: pages 575-576);

Mandelbaum in view of Nishiwaki discloses all the limitations of claim 1. Mandelbaum in view Nishiwaki does not disclose certificate being sent as an independently verifiable data record.

Schneier discloses that a certificate can be transmitted between users for verification. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneir with those of Mandelbaum in view of Nishiwaki and have a certificate sent as an additional independently verifiable data record so that further verification can be provided and/or a public key of a user can be extracted.

Claims 21-37, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in view of Schneier in further view of Carman, U.S. Patent No. 6,272,632.

As per claim 21, the applicant describes a method of delivering a digital document to an intended recipient at a printout station comprising the following limitations which are met by Mandelbaum in view of Schneier:

a) obtaining a first token of each intended recipient (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53; Carman: Col 19, line 62 to Col 20, line 3);

b) encoding the digital document with a session key using a lightweight symmetric cryptographic encryption algorithm, and encrypting the session key with the first token using an encryption algorithm that is more computationally intensive than the symmetric cryptographic encryption algorithm (Schneier: page 33);

c) receiving and securely retaining the digital document, the encrypted session key and an independently verifiable data record of each intended recipient (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53);

d) requesting proof of each intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53);

e) receiving proof of each intended recipient's identity in the form of a second token uniquely related to the first token (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53);

f) decrypting the encrypted session key with the second token, decoding the digital document with the decrypted session key, and releasing the document (Mandelbaum: Col 6, lines 40-44; Schneier: page 33);

g) the receiving step comprises receiving a plurality of transmitted independently verifiable data records of the intended recipients at the printout station (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53);

h) the obtaining step comprises obtaining the first tokens of each of the intended recipients (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53);

i) the requesting step comprises requesting proof of each of the intended recipients' identities at the printout station using data in the independently verifiable data records of the intended recipients (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53);

j) the processing step comprises processing each of the intended recipients' response to the request and releasing the document when all of the intended recipients have proved their identity by use of respective second tokens that are each uniquely related to respective ones of the first tokens (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53);

Mandelbaum discloses the above limitations with the exception that Mandelbaum does not disclose the use of encrypting a session key with a first token. Schneier discloses encrypting a session key with a first

token in order to establish secure communication through the session key. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneier with those of Mandelbaum and utilize a session key because doing so enhances security in the system.

Mandelbaum in view of Schneier does not disclose obtaining a plurality of first tokens. Mandelbaum in view of Schneier discloses obtaining only a first token of a single recipient. Carman discloses the idea of obtaining a plurality of first tokens (public keys) to encrypt a message so that a plurality of entities are necessary to play a part in the decryption. Combining the ideas of Carman with Mandelbaum in view of Schneier allows for a message to be encrypted in more than one first token. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Carman with those of Mandelbaum in view of Schneier for the purpose of creating an environment which is more secure because it depends on more than one entity providing verification for a received message.

As per claims 22-37, the applicant describes the method of claim 21, which is met by Mandelbaum in view of Schneier in further view of Carman, with the following limitation which is met by Mandelbaum:

Wherein the transmitted document is a fax document and the printout station comprises a fax machine (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53).

As per claim 39, the applicant describes the method of claim 21, which is anticipated by Mandelbaum in view of Schneier in view of Carman, with the following additional limitation which is also met by Schneier:

Wherein the transmitted document or a session encryption/decryption key of the transmitted document has been sequentially encrypted with each of the first tokens of the intended recipients in a given order and the processing step comprises sequentially decrypting the transmitted document or a session encryption/decryption key with each of the second tokens of the intended recipients in the reverse of the given sequential order (Col 19, line 62 to Col 20, line 3).

Claims 57 and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in view of Schneier.

As per claims 57 and 63, the claims are rejected under Mandelbaum in view of Schneier for the same reasons given in the rejection of claim 12 (see above).

Claims 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in further view of Carman.

As per claim 40, the applicant describes a method of delivering a digital document which is met by Mandelbaum (see the rejection for claim 1) with the additional limitation of incorporating the use of a plurality of intended recipients which is met by Carman (Col 19, line 62 to Col 20, line 3).

Claim 59 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in view of Auerbach, European Patent Application Publication No. 0798892 A2.

As per claim 59, the applicant describes the method of claim 58, which is met by Mandelbaum, with the following limitation which is met by Auerbach:

Wherein the encoding/decoding steps comprise using enveloping encryption/decryption techniques (Auerbach: Col 3, lines 5-10; Col 3, lines 26-30);

Mandelbaum describes all the limitations of claim 58. However, Mandelbaum fails to disclose the use of enveloping encryption and decryption techniques.

Auerbach discloses a method for the creation and distribution of digital documents using the methods and techniques of secure cryptographic envelopes (Col 1, lines 3-8). Cryptographic envelopes provide an extra layer of security for messages because they comprise superencrypting a message. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Auerbach with those of Mandelbaum so that the transmitted message is encoded using enveloping technique for extra security.

Response to Arguments

Applicant's arguments, see Remarks, filed 10/17/05, with respect to the 112 rejection of claim 21 have been fully considered and are persuasive. The 112 rejection has been withdrawn.

Applicant's arguments with respect to the rejection of claims 1,21, and 41 under Chan have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments with respect to claim 40 have been fully considered but are moot in light of the fact that claim 40 was not rejected under a 102 rejection with Chan.

Applicant's arguments with respect to claim 54 have been fully considered but are not persuasive. The applicant argues that Chan does not teach the limitation of "receiving and securely retaining a transmitted document". This argument is discussed on page 2 of the Remarks as a substantially similar limitation is present in claim 1. The applicant asserts that Chan does not securely retain a transmitted document because in Chan the document is stored in temporary buffer memory. The examiner disagrees with applicant's assertion. Chan clearly discloses retaining a document at the printout station in accordance with a security process; hence Chan discloses "securely retaining a transmitted document at the printout station" as claimed. Nowhere in the claimed invention does the applicant preclude using buffer memory. Accordingly, it seems the applicant is making arguments outside the scope of the claimed invention.

The applicant also argues that Chan does not disclose "determining prior to transmission of the document whether the second station is one which is arranged to implement the present method". This argument fails to comply with 37 CFR 1.111(b) because it amounts to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Applicant's arguments with respect to the rejection of claims 1 and 41 under Mandelbaum have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments with respect to claims 54 (Remarks page 8-9) and claims 40,41, and 49 (Remarks page 9) fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Conclusion

This action is made non-final.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER